

AMENDMENTS TO THE CLAIMS

This Listing of Claims will replace all prior versions and listings of claims in this application.

Listing of Claims:

1. (Currently Amended) A central encryption management system, comprising:
~~an encryption apparatus which can be connected between a plurality of data communications terminals, the plurality of communications terminals for performing data communications;~~
~~the encryption apparatus including encryption/decryption means for performing at least one of an encrypting process and/or a decrypting process on data to terminate encryption-based security between the communications terminals having the encrypting capability and the non-encrypting capability; and~~
~~a manager terminal for inputting information into each of the encryption apparatus and the communications terminals having encrypting capability, the information including whether or not data packets are to be discarded between specific communication terminals after the data packets have been received and a time period for encryption for the presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key into each of the encryption apparatus and the communications terminals remotely from the manager terminal over a network, so that thereby completing settings for the encrypted data communications on each of the apparatus and the communications terminals having encrypting capability are completed;~~
~~wherein the various information includes at least one of instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received; and the time period for the encryption;~~
~~wherein the plurality of communications terminals, the manager terminal, and the encryption apparatus are connected via a cable or wireless network;~~

wherein the encryption apparatus further includes a bridge means for allowing to output data received on one of a plurality of ports of the encryption apparatus to be outputted as it is from another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process; and

wherein the data is received with one of a plurality of ports of the encryption apparatus and the encrypting or decrypting process is performed on the data.

2. (Currently Amended) The central encryption management system according to claim 1, wherein the encryption/decryption means performs the encrypting process and the decrypting process on data, so that wherein the encryption apparatus receives and retransmits is configured to receive and retransmit data in the form of encrypted data from and to one of the plurality of communications terminals having the encrypting capability, and the encryption apparatus is configured to receive and retransmit receives and retransmits the data in the form of non-encrypted data from and to one of the plurality of the communications terminals having no encrypting capability.

3. (Canceled)

4. (Currently Amended) The central encryption management system according to claim 1, wherein:

the encryption apparatus further includes a storage setting information storage means for storing to store the information inputted from the manager terminal, in which the inputted information being is used when controlling the encrypting process and the decrypting process; and

the encryption apparatus controls the encrypting process and the decrypting process by comparing the information stored in the storage setting information storage means with header information of a data packet of the data received with through one of the plurality of ports.

5. (Currently Amended) A central encryption management system, comprising:

an encryption apparatus having a plurality of ports which can be connected between a plurality of communications terminals having either encryption capabilities or no encryption capabilities, in which the encryption apparatus performs at least one of an encrypting process or a decrypting process on data which has been received at one of a plurality of ports after passing through a data link layer and a physical layer; and,

wherein the encryption apparatus outputs the encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled; and

a manager terminal for inputting information, including at least information for instructing whether or not data packets are to be discarded between specific communications terminals after the data packets have been received and a time period for encryption, for the presence or absence of encryption/decryption process, the availability of packet communications, the encryption level, the time period to perform encryption, the encryption policy, and the encryption key, into each of the encryption apparatus and the communications terminals having encryption capabilities remotely from the manager terminal over a network, thereby completing so that a setting of each of the apparatus and communications terminals having encryption capabilities for communicating encrypted data is completed{,};

wherein the various information includes at least one of instructing whether or not data packets are to be discarded between specific terminals after the data packets have been received, and the time period for the encryption;

wherein the plurality of communications terminals, the encryption apparatus, and the manager terminal are configured to be connected via a cable or wireless network.

6. (Currently Amended) The central encryption management system according to claim 5, wherein:

the encryption apparatus further includes setting information storage means for storing a storage to store the information inputted from the manager terminal, in which the inputted information is used when controlling the encrypting process and the decrypting process; and

the encryption apparatus controls the encrypting process and the decrypting process by comparing the information stored in the ~~setting information storage means~~ with header information of a data packet of the data received ~~through~~ with one of the plurality of ports.

7. (New) The central encryption management system according to claim 1, wherein the information comprises at least one of information associated with the presence or absence of encryption or decryption process, the availability of packet communications, an encryption level, a time period to perform encryption, a encryption policy, or an encryption key.
8. (New) The central encryption management system according to claim 1, wherein the plurality of communications terminals are inside a secured network.
9. (New) The central encryption management system according to claim 1, wherein the at least one of the plurality of communications terminals is outside a secured network.
10. (New) The central encryption management system according to claim 1, wherein the encryption apparatus comprises a data path for a connected terminal and performs the encryption process or the decryption process on data received or transmitted on each data path using a different encryption key associated with the connected terminal.
11. (New) The central encryption management system according to claim 1, wherein the plurality of communications terminals having encrypting capability are connected to the encryption apparatus through an access point.
12. (New) The central encryption management system according to claim 1, wherein the plurality of communications terminals are arranged in a plurality of local area networks.
13. (New) The central encryption management system according to claim 12, comprising a plurality of manager terminals, each of the plurality of manager terminals to manage encryption and decryption settings in the communications terminals having encrypting capabilities in at least one of the plurality of local area networks.

14. (New) A method of a central encryption management system, comprising:
receiving data in an encryption apparatus configured to be connected between a plurality of communications terminals having either encryption capabilities or no encryption capabilities;
performing, by the encryption apparatus, at least one of an encrypting process or a decrypting process on data to terminate encryption-based security between the communications terminals having the encrypting capability and the non-encrypting capability; and
bridging data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus without any routing process after the encrypting or decrypting process, wherein
information including whether or not data packets are to be discarded between specific terminals after the data packets have been received and a time period for the encryption are inputted into each of the encryption apparatus and the communications terminals having encrypting capability, thereby completing settings for encrypted data communications on each of the apparatus and the communications terminals having encryption capabilities.

15. (New) The method according to claim 14, comprising:
receiving and retransmitting, by the encryption apparatus, encrypted data from and to one of the plurality of communications terminals having the encrypting capability; and
receiving and retransmitting, by the encryption apparatus, non-encrypted data from and to one of the plurality of communications terminals having no encrypting capability.

16. (New) The method according to claim 14, comprising:
storing, by the encryption apparatus, information inputted from a manager terminal, the inputted information being used when controlling the encrypting process and the decrypting process and
controlling the encrypting process and the decrypting process by comparing the information stored in a storage with header information of a data packet of the data received through one of the plurality of ports.

17. (New) The method according to claim 14, comprising:

performing an encrypting process or a decrypting process on data received at one of the plurality of ports after passing through a data link layer and a physical layer; and
outputting encrypted or decrypted data from another of the plurality of ports through a data link layer and a physical layer associated with the other port without passing said data to a network layer in which routing between networks is controlled.

18. (New) A central encryption management system, comprising:

a plurality of encryption apparatuses configured to be connected between a plurality of communications terminals having no encrypting capability, each of the encryption apparatuses to perform at least one of an encrypting process or a decrypting process on data to terminate encryption-based security between the communications terminals; and

a manager terminal for inputting information including whether or not data packets are to be discarded between specific terminals after the data packets have been received, and a time period for encryption into each of the encryption apparatuses, thereby completing settings for encrypted data communications on each of the encryption apparatuses;

wherein each of the encryption apparatuses further include a bridge to output data received on one of a plurality of ports of the encryption apparatus to another port of the encryption apparatus, without any routing process, after the encrypting or decrypting process.